Protected Information

812.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the Tigard Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the public records information covered in the Records Maintenance and Release Policy.

812.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the Tigard Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

812.2 POLICY

Members of the Tigard Police Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

812.3 RESPONSIBILITIES

The Chief of Police shall select a member of the Department to coordinate the use of protected information.

The responsibilities of this position include but are not limited to:

(a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicle (DMV) records, and Law Enforcement Data System (LEDS).

(b) Developing, disseminating, and maintaining procedures that adopt or comply with the U.S. Department of Justice’s current Criminal Justice Information Services (CJIS) Security Policy.

(c) Developing, disseminating, and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release, and security of protected information.

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

812.4 ACCESS TO PROTECTED INFORMATION

The entire police department is a secure Criminal Justice Agency, where CJIS material is permitted to be retained unlocked, but otherwise secured as necessary, bound by CJIS Security policies. Access to areas of the facility for visitors must be closely controlled, and their unescorted access restricted to those who are performing a required law enforcement action. using the most restrictive set of rights/privelages or access needed by the users for the purposes of specified tasks.

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Tigard Police Department policy or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access that supports a law enforcement action.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution.

812.4.1 ACCESS TO OREGON STATE PATROL OFFENDER INFORMATION

Access to Oregon State Patrol (OSP) criminal offender information may be granted when the information is to be used for the administration of criminal justice, employment, or the information is required to implement a federal or state statute, local ordinance, Executive Order, or administrative rule that expressly refers to criminal conduct and contains requirements or exclusions expressly based on such conduct, or other demonstrated and legitimate needs (OAR 257-010-0025).

812.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Unit to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other department members or the public is at risk. In those instances, cell phones should be used if possible. The transmission should be limited to essential details only, with maximized use of law

enforcement codes (10 or 12 code), concealing information identifying individuals and offenses as much as possible. Plain text transmission of an entire record (summary or full) is prohibited.

Nothing in this policy is intended to prohibit broadcasting warrant information.

812.5.1 REVIEW OF CRIMINAL OFFENDER RECORD

Individuals requesting to review their own Oregon criminal offender information shall be referred to OSP, Identification Services Section (OAR 257-010-0035).

An individual may review his/her local record on file with the Department under the provisions of ORS 192.345(3), and after complying with all legal requirements.

This department will not release information originated by any other agency (ORS 192.311 et seq). Individuals requesting this information shall be referred to the originating agency.

812.6 SECURITY OF PROTECTED INFORMATION

The Chief of Police will select a member of the Department to oversee the security of protected information.

The responsibilities of this position include but are not limited to:

(a) Developing and maintaining security practices, procedures, and training.

(b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents including computer attacks.

(d) Tracking, documenting, and reporting all breach of security incidents to the Chief of Police and appropriate authorities.

812.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

812.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

812.7.1 LEDS TRAINING

All members who operate a terminal to access the LEDS network shall complete a LEDS System Training Guide at a level consistent with the member’s duties. Each member who operates

a terminal to access LEDS must be re-certified by the Department every two years (OAR 257-015-0050).